EXPRESS MAIL NO. EV530953021US

TRANSMITTAL FORM

(To be used for all correspondence after initial filing)

Application Number	10/025,375
Filing Date	December 18, 2001
First Named Inventor	Robert V. M. Oerlemans
Art Unit	2111
Examiner Name	Glenn Allen Auve
Attorney Docket No.	750039.401

ENCLOSURES (*check all that apply*)

- ☐ Fee Transmittal Form
  - ☒ Fee Attached
- ☐ Amendment/Response
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement; Form PTO-1449
- ☐ Cited References
- ☒ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Response to Missing Parts/Incomplete Application
- ☐ Drawing(s)
- ☐ Request for Corrected Filing Receipt
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation, Change of Correspondence Address
- ☐ Declaration
- ☐ Statement under 37 CFR 3.73(b)
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC *(Appeal Notice, Brief, Reply Brief)*
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Return Receipt Postcard
- ☒ Other Enclosure(s) (*please identify below*):

PTOL-85 (+ copy)

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Seed Intellectual Property Law Group PLLC	Customer Number	00500
Signature			
Printed Name	Harold H. Bennett II		
Date	July 25, 2005	Reg. No.	52,404

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature		
Typed or printed name		Date:

Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

00204597.9

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

DEN HAAG, DEN
THE HAGUE, 15/04/05
LA HAYE, LE

Anmeldung Nr:
Application no.: 00204597.9
Demande no:

Anmeldetag:
Date of filing: 19.12.00
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Pijnenburg Custom Chips B.V.
Boxtelseweg 26
5261 NE Vught
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

A data transfer device, a transaction system and a method for exchanging data with a data processing system

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

/00.00.00/

Internationale Patentklassifikation/International Patent Classification/ Classification internationale des brevets:

G06F17/60

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

Title

A data transfer device, a transaction system and a method for exchanging data with a data processing system.

Field of the Invention

The present invention relates, generally, to data communication and, more specifically, to a data transfer device, a transaction system, a method and an Application Specific Integrated Circuit (ASIC) device for exchanging data between remote processing devices.

Background of the Invention

Data storage means, such as chip cards and other electronic data carriers have become increasingly popular for performing financial transactions, for purchasing merchandise, for banking, and other type of data transactions such as for identification and verification purposes.

With the present possibilities for purchasing merchandising, paying bills and the like via the Internet, there is a growing need for completing such transactions using chip cards, credit cards, and the like. However, for this type of "virtual" shopping and banking, security of the transactions is a major problem. This, because a transaction via the Internet involves transmission of data via public, unsecured networks.

U.S. Patent 5.815.577 discloses an encryption module comprising pre-programmed software resident within said module and configured to identify and accommodate a plurality of data input devices, such as scanners, magnetic strip readers, smart card readers, and the like. This module, due to its pre-programmed resident software, fulfils the function of trusted device, such that transactions which are performed through this device can be trusted as to their authenticity. However, this known module has some inherent disadvantages.

Due to the need for pre-programmed software, the device is restricted to operate with data from a known type of chip card of a known transaction entity, such as a bank, for example. Those skilled in

the art will appreciate that this concept is not suitable for the handling of chip cards of transaction entities for which suitable processing software has not been previously incorporated in the device. For adding such software later on, one has to understood that hundreds or even thousands of such trusted devices have to be updated manually in such a case.

This is also true in the case of a change in the processing functions of known chip cards which are supported by the trusted device and for which the already available software in the device has to be updated or even completely revised.

Although it is theoretically feasible to configure the known trusted device for the processing of different chip cards of different transaction entities among others, due to lack of co-operation and standardisation between such transaction entities, in practice, each trusted device operates with a single chip card or other data storage device of a single transaction entity. Accordingly, for each chip card or data storage device a different device has to be installed and used, which leads to an uncomprehensive, impractical and not to manage transaction system.

Although it is feasible to provide the trusted devices with a data receive or download facility, for example for receiving or downloading suitable software for processing new chip cards, a problem arises in the case of transferring this software via common or public data networks, such as the Internet. This, because hackers and others may copy and change the software, such that the security of the trusted device and its proper operation in reading and/or writing data of a data storage device, such as a chip card, can no longer be guaranteed.

Summary of the Invention

It is an object of the present invention to overcome the shortcomings of the prior art.

In accordance with a first aspect of the present invention, a data transfer device is provided, having first data interface means for exchanging data with a data processing system, second data interface means for exchanging data with a user of the data transfer device, and control means for controlling data transfer between the first

and second data interface means, wherein the control means are configured for receiving control data from the first data interface means for selectively enabling data exchange between the first and second data interface means.

Data exchange between the first and second data interface means can be provided, in a further embodiment of the data transfer device according to the invention, such that the control means are configured for enabling part of the second data interface means for operation in a first or open mode.

In a yet further embodiment of the data transfer deceive according to the invention, the control means are configured for enabling the second data interface means for operation in a second or secure mode.

In a preferred embodiment of the data transfer device according to the invention, signalling means are provided for signalling the mode of operation of the data transfer device, that is the open or secure mode. Suitable signalling means comprise a Light Emitting Diode (LED) configured such that the LED is illuminated if the data transfer device is in its secure mode of operation.

By selectively enabling data exchange between the first and second data interface means of the data transfer device in accordance with the present invention, data can be exchanged in an open mode or a secure mode of operation of the data transfer device. In the open mode, the data transfer device is operative for exchanging data with a data processing system not requiring a particular type of security. However, in the secure mode of operation, the data transfer device enables data exchange with a data processing system requiring a degree of security. Accordingly, with the data transfer device according to the invention, both secure and non-secure data exchange can be supported, providing already greatly enhanced data processing capabilities compared to the prior art devices as discussed above.

The control means are configured, in a yet further embodiment of the invention, for processing data provided by the first and second data interface means in accordance with the control data. That is, in this embodiment of the invention, the control means comprise data processing capabilities.

In a preferred embodiment of the data transfer device according to the invention, the control means are configured for processing

data provided by the first and second data interface in accordance with program execution data to be executed by the data processing system, wherein the program execution data is comprised by the control data. That is, part of a program to be executed by the processing system is transferred and performed by the data transfer device. By providing that the program execution data transferred to and running on the data transfer device is genuine or trusted data, data exchange between the first and second data interface means of the data transfer device can be likewise performed in a safe and trusted or secure manner.

In accordance with an embodiment of the invention, the program execution data are only executed by the data transfer device if same is set into its secure mode of operation. With this option, according the present invention, a variety of data provided at the second or user data interface means of the data transfer device can be handled safely and in guaranteed manner by transferring the proper and secure control data to the control means of the data transfer device.

In order to set the device safely and guaranteed in either the secure mode or the open mode, in accordance with a yet further embodiment of the invention, the data transfer device comprises data storage means for storing authentication data, and wherein the control means are configured for providing an authentication check on the received control data for setting the data transfer device in either one of the open and secure mode of operation.

Using control data comprising certificate data, and control data means configured for checking the certificate data of the control data with respect to certificate data stored in the data storage means, the data transfer device is set in its secure mode of operation if the certificate data of the control data are approved and the data transfer device is set in its open mode of operation for either one of disapproval of the certificate data and non-availability of certificate data of the control data, and wherein the control data are deleted if the certificate data thereof are false.

In a preferred embodiment of the invention, the second data interface means comprise keypad means, data card reader means and display means, wherein the control means in the open mode are configured for enabling access to the data card reader means, and wherein the control

means in the secure mode are configured for enabling access to the keypad means, the data card reader means and the display means.

That is, the keypad means and the display means of the data transfer device are only active in the secure mode. Accordingly, the keypad means and the display means are arranged as "secure" or "trusted" devices, with which data can be exchanged and processed requiring a certain degree of security. In the open mode of operation, the keypad means and the display means are not enabled for data transfer.

With the implementation of the authentication check, the data transfer device according to the invention can be easily arranged for supporting data transfer form a plurality of chip cards or other data storage devices, for example, in both the open or secure mode of operation, thereby providing a flexible device suitable for processing data of a plurality of chip cards and the like.

By configuring the data transfer device, in a still further embodiment of the invention, for processing data provided by the card reader in accordance with the control data received, data exchange in accordance with a plurality of functions supported by a chip card can be provided.

In order to enhance the security of the data transfer between the data transfer device and a data processing system, in a yet further embodiment of the invention, the data transfer device comprises means for supporting encrypted data transfer via the first interface means and the data processing system, thereby making the data exchange unreadable without a proper decryption algorithm and/or password.

A further improvement of the security of the data transfer device is provided in a further embodiment thereof, wherein the control means are configured for erasing the control data after each transaction or after a predetermined time period upon completion of a transaction, for example.

The first data interface means may comprise any standardised computer data interface means, such as USB (Universal Standard Bus) interface means, RS 232 interface means which are known to those skilled in the art, and others.

In accordance with a second aspect of the present invention, a transaction system is provided, comprising a first processing device such as to be operated by an authorisation entity, a second

processing device such as to be operated by a user, and a data transfer device in accordance with any of the previous claims, wherein the first and second processing devices connect to a data network, and wherein the data transfer device with its first interface means connects to the second processing device, characterized in that the first and second processing devices are configured for exchanging control data from the first processing to the data transfer device for selectively enabling the second data interface means of the data transfer device.

In the transaction system according to the invention, transaction data between the first and second processing devices are exchanged through the data transfer device of the present invention, which is either set in its open or its secure mode of operation through suitable control data received by the data transfer device.

In the case of a transaction involving the exchange of secure financial data or other trusted data between the first and second processing devices, for example in accordance with a further embodiment of the system according to the invention, the first processing means are configured for providing control data for setting the data transfer device in a secure mode and the first and second processing devices are configured for enabling a transaction after the data have been exchanged.

In a yet further embodiment the transaction system comprises a third processing device such as to be operated by a transaction entity, wherein the third processing device connects to the data network, and wherein the first processing device is configured for enabling a transaction between the second and third processing devices dependent on the enabling of the second interface means of the data transfer device.

That is, suppose a user would like to order merchandise from a store, either a real a store or a virtual store, comprising the third processing means. In order that this transaction will be enabled, the merchandise has to be paid, for which financial data have to be exchanged between the user and a financial entity, such as a bank, comprising the first processing means.

Suppose that the user wishes to pay by using a credit account receding at the financial entity, appropriate financial data have to be exchanged between the user and the financial entity. If the user would like to use a credit card or a chip card or the like, the data transfer device has to be set in a secure mode, operative for processing

the data of the particular card. The financial entity, from its first processing device, provides suitable control data to the data transfer device via the second processing device to which the data transfer device connects. Once in its secure mode, data between the first and second processing devices can be securely exchanged. After the completion of this exchange, the merchandise selling entity will be informed, such that the transaction between the second and third processing devices can be enabled and completed.

Those skilled in the art will appreciate that the transaction system according to the invention is not limited to the exchange of financial data or the purchase of merchandise or the like. In fact, the transaction system according to the invention can be used for any type of transaction wherein the data transfer device operates in either one of its open or secure mode.

In a third aspect of the invention, a method for exchanging data with a data processing system is provided using a data transfer device having first data interface means for exchanging data with the data processing system, second data interface means for exchanging data with a user of the data transfer device and control means for controlling data transfer between the first and second data interface means, which method comprises by the steps of:

- transferring control data from the data processing system to the data transfer device, and
- selectively enabling data transfer between the first and second data interface means of the data transfer device dependent on the control data received.

In a yet further embodiment of the method according to the invention an authentication check is performed on the received control data for setting the data transfer device in its open or secure mode of operation.

For this purpose, according to the invention, the control data comprise certificate data, wherein the control data are checked by the control means with respect to the certificate data, and wherein the data transfer device is set in its secure mode of operation if the certificate data of the control data are approved and the data transfer device is set in its open mode of operation for either one of disapproval of the certificate data and non-availability of certificate

data of the control data, and wherein the control data is deleted if the certificate data thereof are false.

In the open mode, the data transfer device can be arranged for exchanging data with the user via the second data interface means through a limited number of data input means, such as data card reader means, whereas in the secure mode data exchange with a plurality of data input devices connected to the data transfer device is enabled, including keypad means, card reader means, and display means, for example.

In order to enhance the security during exchange of data between the data processing system and the data transfer device, in a further embodiment of the method according to the invention, the data are transferred in an encrypted form.

Maximum security is obtained by erasing the control data in the data transfer device after the completion of a data exchange.

The invention relates also to an Application Specific Integrated Circuit (ASIC) device comprising data exchange means and control means for selectively enabling data exchange between first and second data interface means based on control data in accordance as dislosed above.

In a yet further embodiment of the invention, the ASIC device further comprises at least one of the first and second data interface means, and/or data processing means for processing data provided by the first and second data interface means in accordance with program execution data provided by the control data. The ASIC device further may comprise data storage means, among others for storing the control data, the program execution data and authentication data.

The above-mentioned and other features and advantages of the invention are illustrated in the following description with reference tot the enclosed drawings.

Brief Description of the Drawings

Figure 1 shows, in a schematic and illustrative manner, a block diagram of a data transfer device in accordance with the present invention, connected to a processing device, such as a Personal Computer (PC).

Figure 2 shows, in a schematic and illustrative manner, a transaction system in accordance with the present invention.

Figure 3 illustrates in a schematic manner a method of operation in accordance with the present invention.

Description of the Embodiments

Without the intention of limitation the invention will now be explained by its application with a data transfer device comprising a limited number of user data input and output means.

In figure 1, reference numeral 10 refers to a data transfer device in accordance with the present invention. The data transfer device 10 connects to a Personal Computer (PC) 30 by a standard Universal Serial Bus (USB) or RS 232 data link 50, for example.

The data transfer device 10 comprises first data interface means 11 and second data interface means 12 including keypad means 13, display means 14 and data card reader means 15, such as chip card 48 or magnetic strip card reader means. Those skilled in the art will appreciate that the second data interface means 12 may comprise other well known data input and data output means.

Data transfer between the first and second data interface means 11, 12 is controlled by control means 20 which, for clarity purposes, have been shown in the form of switching means.

In a first or open mode position 21 of the control means 20, data transfer between the first and second data interface means 11, 12 is handled under the control of so-called Unsecured Function Extension (UFE) means 24. In a second or secure mode position 22 data transfer between the first and second data interfaces 11, 12 is controlled by so-called Secure Function Extension (SFE) means 25. The UFE and SFE means 24, 25 are arranged for processing program execution data.

In the open mode, through the UFE means 24, the card reader part 15 of the second data interface means 12 is enabled for the exchange of data with the first data interface means 11. Such as indicated by reference numeral 26.

In the secure mode, the SFE means 25 are configured for enabling data exchange from any of the second data interface means 12, i.e. the keypad means 13, the display means 14 and the card reader means 15. This, as indicated by reference numerals 27, 28 and 29, respectively.

Reference numeral 23 denotes a Light Emitting Diode (LED) for indicating the mode of the data transfer device 10. In the preferred embodiment, the LED 23 is illuminated if the device 10 is in its secure mode. Those skilled in the art will appreciate that signalling means other than a LED may be used for this purpose, for example the display means 14.

The data transfer device 10 further comprises data storage means 16, 17 and 18. In use, the storage means 16 comprise so-called security library program data, among others comprising authentication or certification data for use with the SFE means 25. The storage means 17 comprise user I/O library program data, configured for controlling the Input/Output (I/O) with the keypad means 13 and display means 14 of the second data interface means 12. The storage means 18 comprise data configured for controlling the card reader means 15 of the second data interface means 12. Part of the library data may be provided in a non-volatile memory, such as an EEPROM (Electrically Erasable Programmable Read Only Memory) 19. This data may be used for checking prublic encryption keys on certificate data, for example.

The PC 30 can be a conventional Personal Computer or any other processor controlled device, comprising data interface means 31 for exchanging data with the first data interface means 11 of the data transfer device 10, such as USB or RS 232 data interface means 31. Further, the PC 30 comprises data storage means 32 for storing data, an Application Programming Interface (API) 33 which operates with browser software 34, and application software 35, such as the well-known Java software.

The PC 30 further comprises keyboard means 36, mouse means 37, display or monitor means 38, data input means such as a CDROM interface with the Internet.

The UFE and SFE means 24, 25 are configured for executing program data in conjunction with the application software 35 of the PC 30. That is, the UFE and SFE means functions either as an unsecure extension or a secure extension of the software 35 to be executed in the data transfer device 10.

As schematically indicated, through the data network interface 40 application data is exchanged with an application 60 running on a remote processing device (not shown).

For clarity purposes, the data link 50 comprises a control part 51, a download part 52 and an application part 53.

The control part 51 provides overall control of the data exchange between the data transfer device 10 and the PC 30. The download part 52 is arranged for downloading data into the data transfer device 10 from the PC 30. The application part 53 is operative for controlling the UFE means 24 and the SFE means 25 of the data transfer device 10.

Figure 2 illustrates, in a schematic manner, a typical transaction system according to the present invention.

De data transfer device 10 with its keypad means 13, display means 14, card reader means 15 and signalling means 23 connects via its first interface means 11 and the data link 50 to a processing device such as PC 30, to be operated by a user of the transaction system.

As illustratively indicated, the PC 30 connects via an Interface 40 and a modem or other suitable data link connection device 41 to a data network such as the Internet 49.

Further a, transaction entity having a processing device 42 connects to the Internet 49, for example a grocery shop either a real or a virtual shop, for selling merchandise or goods 43.

An authorisation or authentication entity having a processing device 44, such as a bank or clearing house, likewise connects to the Internet 49.

For the sake of clarity, in the following description, it is assumed that data between the processing devices 30, 42 and 44 is exchanged via known and/or standardised communication protocols, which are well known to those skilled in the art, such that no further description thereof has to be provided here.

With reference to Figure 3, it is now assumed that a user of the PC 30 and the data transfer device 10 intends to purchase merchandise 43 of the shop via its processing device 42.

Generally, once the user of the PC 30 has made his choice as to the merchandise 43 to be purchased, a financial transaction has to be performed using a credit card 48, associated with an account 45 at the bank or authorisation entity having the processing device 44.

To this end, the user of the PC 30 contacts the processing device 44 in order to have the financial transaction enabled. As a first input, the user of the PC 30 indicates the type of credit card

he intends to use for completing the financial transaction. It will be understood that the type of credit card to be used can be prescribed by the processing device 42 of the shop selling the merchandise 43.

Because of the secure nature of the financial transaction, the processing device 44 of the authorisation entity transmits certified SFE program execution data 46 to the transfer device 10 via the Internet 49. Upon receipt of this SFE program execution data 46, the SFE control means 25 check weather this SFE control data 46 is certified control data, which can be safely loaded into the SFE means 25.

In the affirmative, the control means 20 of the transfer device 10 operate in order to set the transfer device 10 in its secure mode, enabling the keypad means 13, the display means 14 and the card reader means 15, while at the same time the LED 23 is illuminated. The certification or authentication check is provided through the security program library 16 of the data transfer device 10.

If the authentication check fails, due to disapproval of the certificate data or if no certificate data are available at all, the data transfer device is set in its open mode of operation. The control data, i.e. the program execution data received in the data transfer device 10 are deleted if said certificate data are false. In the latter case, no data exchange via the second data interface means 12 of the data transfer device 10 is permitted.

Once in its secure mode, data exchange via the transfer device 10, i.e. its keypad 13, the display means 14 and the card reader means 15 can be regarded as trusted data, such that transactions involving the account 45 at the processing device 44 of the bank or authorisation entity can be safely amended. For example, a money transfer from the account 45 of the user to the account of the entity selling the merchandise 43.

The program execution data loaded into the SFE means 25 provide the interaction with and the processing of the data exchange via the card reader means 15. That is, data form the card 48 are processed by the SFE means 25 in accordance with the program execution data loaded through the second data interface means 12 and the control means 20 of the data transfer device 10. In this manner an entity providing a data card can be shure that the card is treated in accordance with pre-defined steps and procedures, approved bij this entity.

Once the transaction has been completed, the secure data change via the data transfer device 10 can be closed, while the processing device 44 of the authorisation entity can inform the processing device 42 of the vendor of the merchandise 43 of the successful completion of the transaction. Accordingly, the merchandise 43 can be delivered with the user.

Dependent on the type of application 60, id. purchasing merchandising, purchasing services, banking or other transactions, difference SFE data 46 can be exchanged with the data transfer device 10, providing a flexible as possible transaction system. It is noted that the program execution data 46, also called 'Smartlets' may comprise data for processing the data from the keypad means 13 and/or the card reader means 15 in accordance with a particular data processing function. This data processing function may also be contained in the data on the chip card 48.

In those cases wherein no secure transaction has to be performed, the processing device 44 will transmit UFE program or control data, setting the data transfer device 10 in its open mode. In this mode, the device 10 is configured for exchanging data from the chip card 48 only and in accordance with an open, standard transaction procedure.

Accordingly, with the transaction system of the present invention, multiple data cards or chip cards can be processed in either a secure or an open mode of operation, there by providing a flexible data transfer system.

Although the transaction system and method according to the invention have been disclosed by reference to its use via the Internet 49, those skilled in the art will appreciate that any other data network for the transfer of data can be used, such as a direct link with the processing devices 42 and/or 44.

Further, the transaction system in accordance with the invention is both suitable for use at home and/or in shops or the like, for handling secure and/or open data transactions with a plurality of data storage devices, not limited to chip cards, magnetic strip cards and the like.

In order to enhance the security of the data transaction, after completion thereof the program data 46 or 'Smartlets' can be erased in the data transfer device 10, for example with the

withdrawal of the chip card 48. This, in order to avoid that the control data can be extracted from the data transfer device 10. Further, the secure transactions and, of course, also the open transactions, can be performed using any type of encryption of the data exchange between the several processing devices 30, 42 and 44.

The invention further relates to an Application Specific Integrated Circuit (ASIC) device comprising any or a selction of the control means 20, the SFE and UFE means 24, 25, the storage means 16, 17, 18 and the data interface means 11. Such an ASIC provides enhanced security to the data transfer device 10 as a whole.

Various modifications in the design and implementation of the various components and method steps discussed above may be made without departing from the spirit and scope of the invention, as set forth in the appendent claims.

(100)

Claims

1. A data transfer device, having first data interface means for exchanging data with a data processing system, second data interface means for exchanging data with a user of said data transfer device, and control means for controlling data transfer between said first and second data interface means, characterised in that said control means are configured for receiving control data from said first data interface means for selectively enabling data exchange between said first and second data interface means.

2. A data transfer device according to claim 1, wherein said control means are configured for processing data provided by said first and second data interface means in accordance with said control data.

3. A data transfer device according to claim 2, wherein said control means are configured for processing data provided by said first and second data interface in accordance with program execution data to be executed by said data processing system, wherein said program execution data is comprised by said control data.

4. A data transfer device according to claim 1, 2 or 3, wherein said control means are configured for enabling part of said first and second data interface means for operation in a first or open mode.

5. A data transfer device according to claim 1, 2 or 3, wherein said control means are configured for enabling said second data interface means for operation in a second or secure mode.

6. A data transfer device according to claim 5, wherein said control means are configured for executing said program data if said data transfer device is set in its secure mode of operation.

7. A data transfer device according to claim 2, 3, 4, 5 or 6, further comprising data storage means for storing authentication data, and wherein said control means are configured for providing an authentication check on said received control data for setting said data transfer device in either one of said open and secure mode of operation.

8. A data transfer device according to claim 7, wherein said control data comprise certificate data, and wherein said control data means are configured for checking said certificate data of said control data with respect to certificate data stored in said data storage means, for setting said data transfer device in its secure mode of operation if

said certificate data of said control data are approved and for setting said data transfer device in its open mode of operation for either one of disapproval of said certificate data and non-availability of certificate data of said control data, and for deleting said control data if said certificate data thereof are false.

9. A data transfer device according to claim 4, 5, 6, 7 or 8, wherein said second data interface comprises keypad means, data card reader means and display means, wherein said control means in said open mode are configured for enabling access to said data card reader means, and wherein said control means in said secure mode are configured for enabling access to said keypad means, data card reader means and display means.

10. A data transfer device according to claim 9, wherein said control means are configured for processing data provided by said card reader in accordance with said control data received.

11. A data transfer device according to any of the claims 4, 5, 6, 7, 8, 9 or 10, further comprising signalling means for signalling said mode of operation of said data transfer device.

12. A data transfer device according to claim 11, wherein said signalling means comprise a Light Emitting Diode (LED), and wherein said control means are arranged for illuminating said LED if said data transfer device is in its secure mode of operation.

13. A data transfer device according to any of the previous claims, further comprising means for supporting encrypted data transfer via said first interface means.

14. A data transfer device according to any of the previous claims, wherein said first data interface means comprise standardised computer data interface means, such as USB (Universal Serial Bus) interface means.

15. A transaction system, comprising a first processing device such as to be operated by an authorisation entity, a second processing device such as to be operated by a user, and a data transfer device in accordance with any of the previous claims, wherein said first and second processing devices connect to a data network, and wherein said data transfer device with its first interface means connects to said second processing device, characterised in that said first and second processing devices are configured for exchanging control data from said first

processing to said data transfer device for selectively enabling said second data interface means of said data transfer device.

16. A transaction system according to claim 15, wherein said transaction involves exchange of trusted data, wherein said first processing device is configured for providing control data for setting said data transfer device in a secure mode.

17. A transaction system, according to claim 15 or 16, comprising a third processing device such as to be operated by a transaction entity, wherein said third processing device connects to said data network, and wherein said first processing device is configured for enabling a transaction between said second and third processing devices dependent on said enabling of said second interface means of said data transfer device.

18. A transaction system according to claim 17, wherein said transaction between said second and third processing devices involves exchange of trusted data between said first and second processing devices, wherein said first processing device is configured for providing control data for setting said data transfer device in a secure mode and wherein said third processing device is configured for enabling said transaction between said second and third processing devices after said trusted data have been successfully exchanged.

19. A transaction system according to claim 17 or 18, comprising a plurality of first, second and third processing devices, wherein said data network is a public data network, such as the Internet.

20. A first processing device configured for operating in accordance with any of the claims 14, 15, 16, 17, 18 or 19.

21. A second processing device configured for operating in accordance with any of the claims 14, 15, 16, 17, 18 or 19.

22. A third processing device configured for operating in accordance with any of the claims 14, 15, 16, 17, 18 or 19.

23. A method of exchanging data with a data processing system using a data transfer device having first data interface means for exchanging data with said data processing system, second data interface means for exchanging data with a user of said data transfer device, and control means for controlling data transfer between said first and second data interface means, characterised by the steps of:

- transferring control data from said data processing system to said data transfer device, and

- selectively enabling data exchange of data between said first and second data interface means.

24. A method according to claim 23, wherein data provided by said first and second data processing means is processed in accordance with program execution of a program executed by said data processing system, said program execution data being comprised by said control data.

25. A method according to claim 23 or 24, wherein an authentication check is performed by said control means on said control data for setting the data transfer device in either one of an open and secure mode of operation.

26. A method according to claim 25, wherein said control data comprise certificate data, wherein said control data are checked by said control means with respect to said certificate data, and wherein said data transfer device is set in its secure mode of operation if said certificate data of said control data are approved and said data transfer device is set in its open mode of operation for either one of disapproval of said certificate data and non-availability of certificate data of said control data, and wherein said control data is deleted if said certificate data thereof are false.

27. A method according to claim 26, wherein said data transfer device in its open mode of operation exchanges data with said second data interface means through a limited number of data input means thereof, such as a data card reader means, whereas the data transfer device in its secure mode of operation exchanges data with said second data interface means through a plurality of data input and output devices thereof, including keypad means, display means, and card reader means.

28. A method according to claim 23, 24, 25, 26 and 27, wherein data between said data processing system and said data transfer device are exchanged in an encrypted form.

29. A method according to claim 23, 24, 25, 26, 27 and 28, wherein control data in said data transfer device are erased after the completion of a data exchange.

30. An Application Specific Integrated Circuit (ASIC) device comprising data exchange means and control means for selectively enabling

data exchange between first and second data interface means based on control data in accordance with any of the previous claims.

31. An ASIC device according to claim 30, further comprising at least one of said first and second data interface means.

32. An ASIC device according to claim 30 or 31, further comprising data processing means for processing data provided by said first and second data interface means in accordance with program execution data provided by said control data.

33. An ASIC device according to claim 30, 31 or 32, further comprising data storage means, among others for storing said control data, said program execution data and authentication data.

Abstract

(100)

A data transfer device (10), having first data interface means (11) for exchanging data with a data processing system (30), second data interface means (12) for exchanging data with a user of the data transfer device, and control means (20) for controlling data transfer between the first and second data interface means (11, 12). The control means (20) are configured for receiving control data from the first data interface means (11) for selectively enabling data exchange between the first and second data interface means (11, 12). The control means (20) can be configured for enabling part of the first and second data interface means (11, 12) for operation in a first or open mode, and for enabling the second data interface means (12) for operation in a second or secure mode of operation.

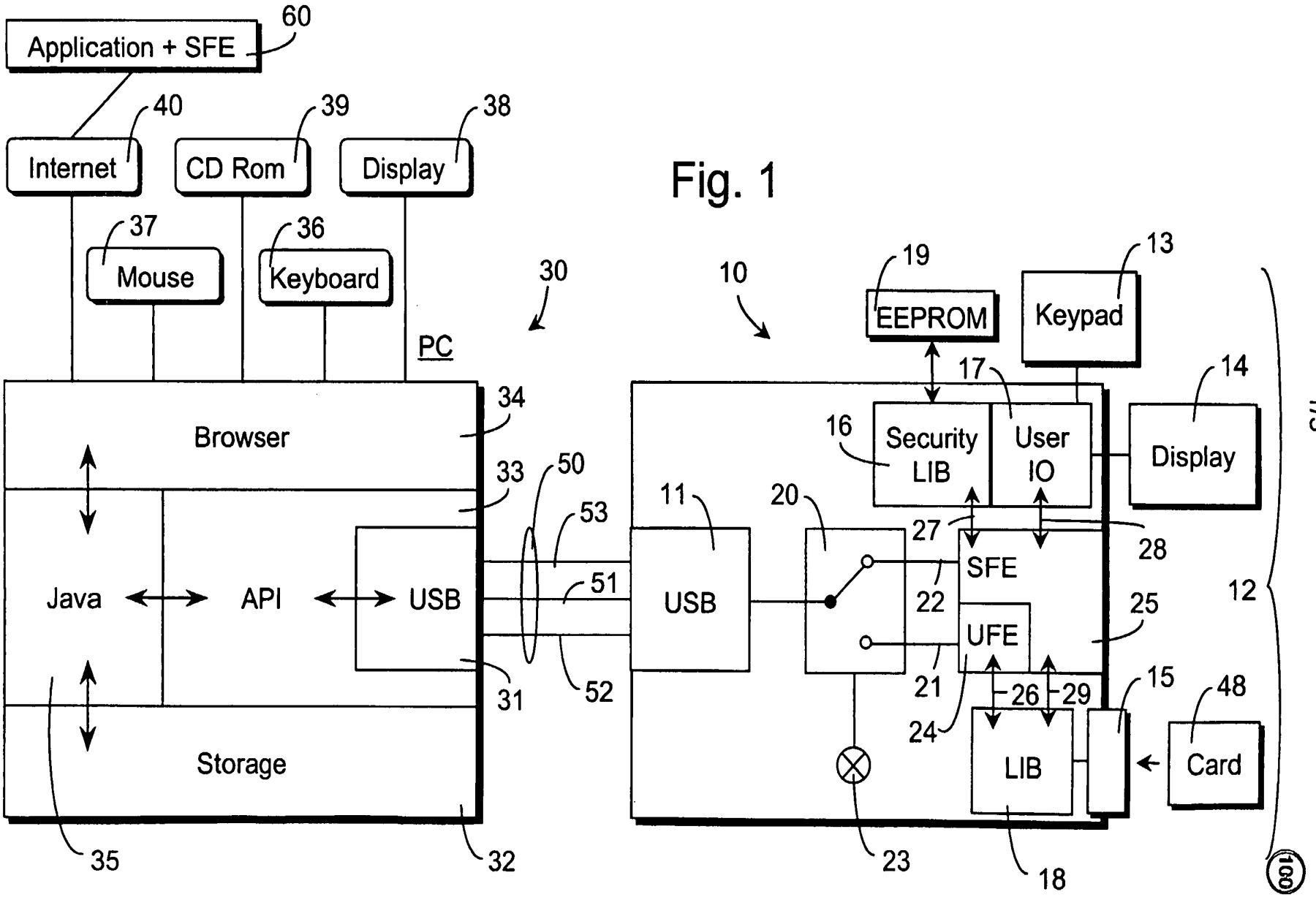

Fig. 1

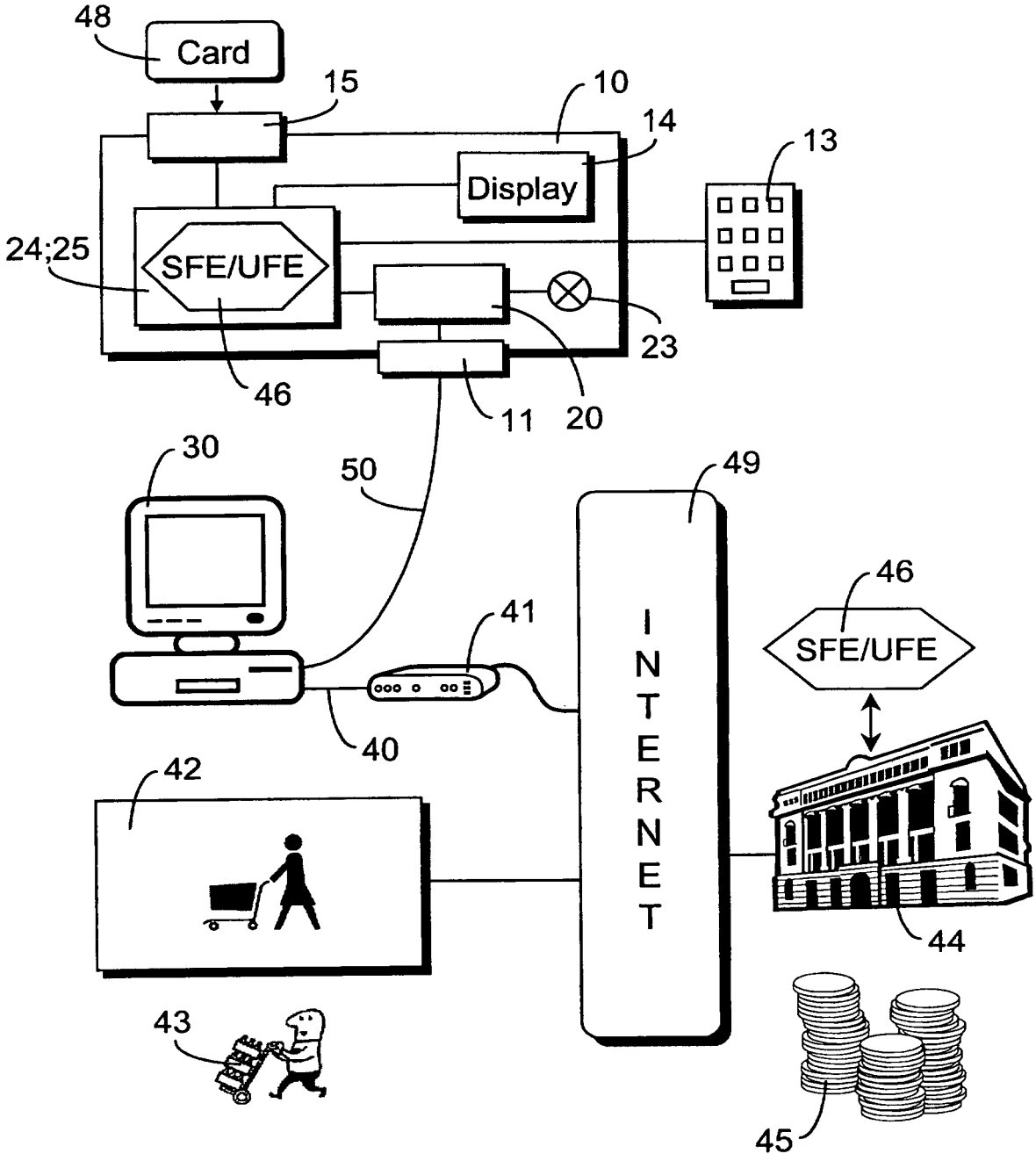
48
Card
15
10
14
13
Display
24;25
SFE/UFE
23
46
11
20
30
50
49
46
41
INTERNET
SFE/UFE
40
42
44
43
45

Fig. 2

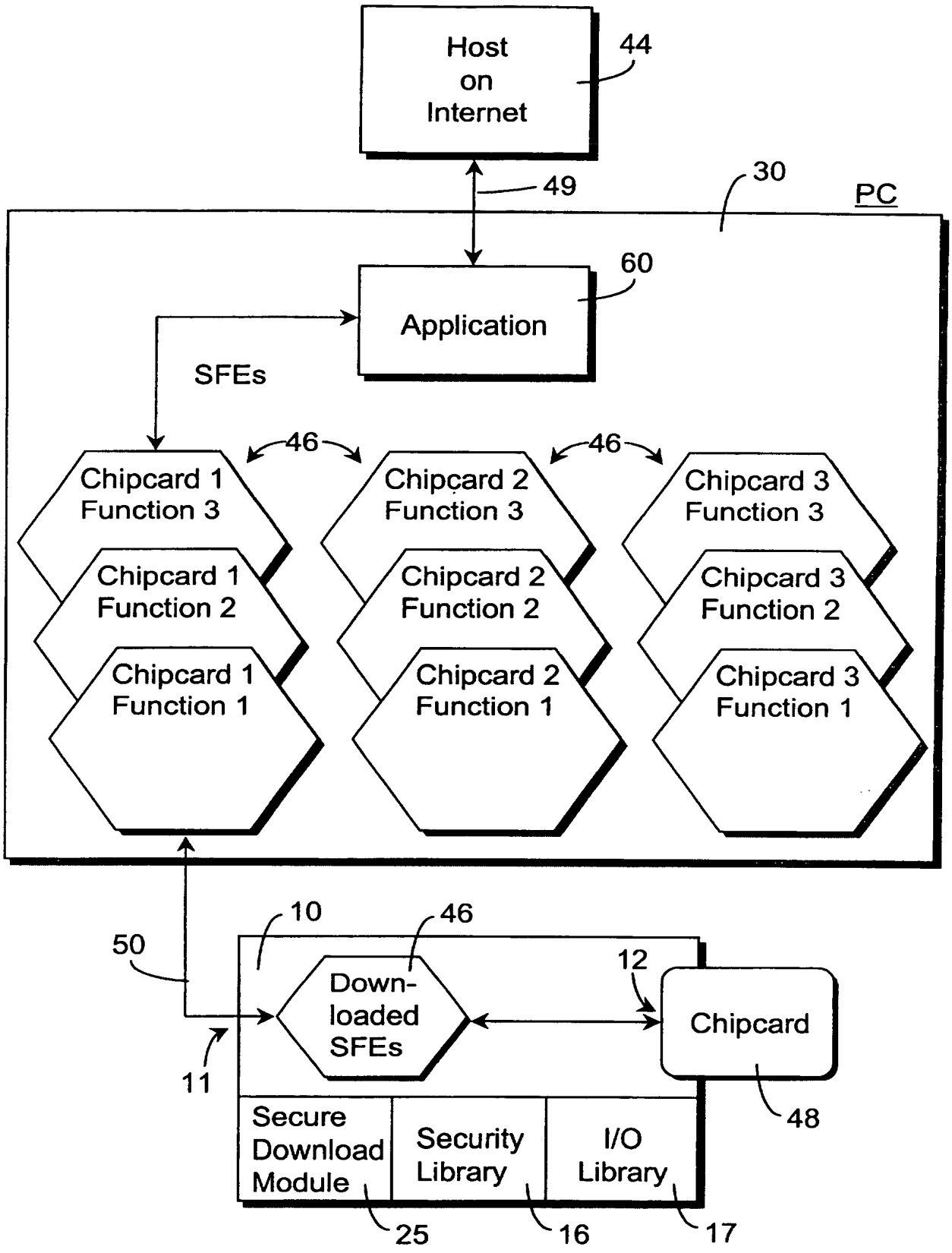
Host
on
Internet
44
49
30
PC
60
Application
SFEs
46
46
Chipcard 1
Function 3
Chipcard 1
Function 2
Chipcard 1
Function 1
Chipcard 2
Function 3
Chipcard 2
Function 2
Chipcard 2
Function 1
Chipcard 3
Function 3
Chipcard 3
Function 2
Chipcard 3
Function 1
10
46
50
12
Down-
loaded
SFEs
Chipcard
11
48
Secure
Download
Module
Security
Library
I/O
Library
25
16
17

Fig. 3